REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-05-2012	FINAL	

4. TITLE AND SUBTITLE

USCYBERCOM: Right Solution, Wrong C2 Structure

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Daniel C. Wood, II

Paper Advisor: LtCol Antonio Morabito

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The emergence of *cyberspace* as the fifth operational domain of warfare and the related disorganized efforts to conduct operations within it resulted in the Department of Defense (DoD) standing up United States Cyber Command (USCYBERCOM) as a subordinate unified command under United States Strategic Command (USSTRATCOM) to focus these efforts. However, a subordinate unified command structure contains inherent impediments that unnecessarily hinder the CDRUSCYBERCOM in the prosecution of his mission to accomplish his specified operational objectives. This work assesses the limitations and the nuances that impede the CDRUSCYBERCOM as a subordinate unified commander in the accomplishment of his objectives and recommends change to USCYBERCOM *command organization*. In order for USCYBERCOM to better accomplish its operational objectives, USCYBERCOM must transition to a unified command because its mission and complex operational environment combined with the consideration of operational factors of time, space, and force bring about a confluence of factors that require unified command authority to do so.

15. SUBJECT TERMS

Command Organization, Command and Control, Cyberspace Operational Environment

16. SECURITY CLASSIFICATION OF: **UNCLASSIFIED**			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		**22**	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

USCYBERCOM: RIGHT SOLUTION, WRONG C2 STRUCTURE

by

Daniel C. Wood, II
MAJ USA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

04 MAY 2012

Abstract

The emergence of *cyberspace* as the fifth operational domain of warfare and the related disorganized efforts to conduct operations within it resulted in the Department of Defense (DoD) standing up United States Cyber Command (USCYBERCOM) as a subordinate unified command under United States Strategic Command (USSTRATCOM) to focus these efforts. However, a subordinate unified command structure contains inherent impediments that unnecessarily hinder the Commander of USCYBERCOM (CDRUSCYBERCOM) in the prosecution of his mission to accomplish his specified operational objectives. This work assesses the limitations and the nuances that impede the CDRUSCYBERCOM as a subordinate unified commander in the accomplishment of his objectives and recommends change to USCYBERCOM *command organization*. In order for USCYBERCOM to better accomplish its operational objectives, USCYBERCOM must transition to a unified command because its mission and complex operational environment combined with the consideration of operational factors of time, space, and force bring about a confluence of factors that require unified command authority to do so.

Table of Contents

Introduction	1
Emergence of a New Operational Domain of Warfare	3
USCYBERCOM Mission and Operational Environment	5
Considering Time, Space and Force Implications and Impediments	10
Counterargument	15
Summary/Recommendations	17
Bibliography	18

Introduction

> "DoD has a large IT footprint. We operate more than 15,000 networks within the .mil domain. We have seven million computing devices. 90,000 people are directly involved in the operation of our information technology. We rely not only on our own networks, but also on many commercial and government networks outside the .mil domain. The fact is that our department depends on the overall IT infrastructure of our nation. The threat to our computer networks is substantial. They are scanned millions of times a day. They are probed thousands of times a day. And we have not always been successful in stopping intrusions. In fact, over the past several years we have experienced damaging penetrations."[1]

The foregoing statement provided by former Undersecretary of Defense William Lynn alludes to the magnitude of a complex problem facing the U.S. Department of Defense (DoD) – the criticality *of* and unfortunate vulnerabilities *in* the heavily relied upon technological underpinnings of its defense forces. From the interconnected terrestrial and satellite based communication pathways that facilitate national level command and control to the ability for a dismounted individual Soldier, Sailor, Airman or Marine to navigate individually or in their various platforms via data transmitted from space by the Global Position System, essentially everything the U.S. DoD does is reliant upon robust, persistent, and reliable communication networks. President Obama makes this poignantly clear in current U.S. National Security Strategy, "Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority."[2]

Having full operational capability on October 21, 2010 as a subordinate unified command under United States Strategic Command (USSTRATCOM), USCYBERCOM is now the DoD's primary component for this effort and answer to the problem of defending its

[1] Under Secretary of Defense William J. Lynn, III, speech given on May 22nd, 2010 at the STRATCOM Cyber Symposium, Omaha, NE, available at http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1, accessed March 12, 2012.
[2] President Barrack Obama, 2010 National Security Strategy, P. 28.

networks and taking offensive action against adversaries in cyberspace.[3] However, USCYBERCOM's operational *command organization* as a subordinate unified command under USSTRATCOM brings about inherent impediments to its ability to accomplish its specified objectives included in its mission statement: "…USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations…".[4]

This work assesses the limitations and the nuances that impede the CDRUSCYBERCOM as a subordinate unified commander as he prosecutes his mission toward the accomplishment of his objectives. Research demonstrates how the following interrelated factors impede the commander and demonstrate the need for USCYBERCOM to become a unified command: the impediments created by the unique and complex operational environment and the impediments resulting from the operational factors of time, space, and force regarding the USCYBERCOM mission – particularly plaguing is the disparity between combatant command authority, held by unified commanders, and operational control, held by subordinate unified commanders. In order for USCYBERCOM to better accomplish its operational objectives, USCYBERCOM must transition to a unified command because its mission and complex operational environment combined with the consideration of operational factors of time, space, and force bring about a confluence of factors that require unified command authority to do so. As a basis, one must have an understanding of the development and complexity of cyberspace, the USCYBERCOM mission and the

[3] United States Strategic Command Fact Sheet, available at http://www.stratcom.mil/factsheets/Cyber_Command/, accessed March 13, 2012.
[4] Ibid.

operational environment in which USCYBERCOM attempts to achieve its objectives, as well as the operational factors as they relate to cyberspace operations.

Emergence of a New Operational Domain of Warfare

Armed conflict has brought about advances in almost every sector of daily life – from advances in sea, air, land and space platforms to information technology. As early as the American Civil War, information technology and its uses entered the operational environment. Though the *Blue* and *Gray* tactical formations relied upon a system based on the movements of large flags waved by Soldiers to send messages, at the operational and strategic levels, line-of-sight communications proved insufficient to facilitate timely communications over the vast distances involved. New information technologies began to permeate command centers based on the work of many including Samuel B. Morse. In 1844, Morse sent the first telegraph message from Boston to Washington and by 1862 President Abraham Lincoln used the recently invented *telegraph* to communicate to his operational commanders in the field. "'What became of our forces which held the bridge till twenty minutes ago…?', the President of the United States telegraphed a colonel in the field during the Civil War Battle of Second Manassas (Bull Run)..."[5]

In essence, while there was no terminology for it at the time, when Samuel B. Morse sent the first telegraph message from Baltimore to Washington, D.C. in 1844, the first digital communication network was created and the foundation for *cyberspace* was born – ultimately developing into myriad networks that now comprise much more than that which we commonly refer to as the *INTERNET* today. Not until 1984, though, did the term *cyberspace* first appear in print – in the novel *Neuromancer*, by William Gibson, wherein

[5] Tom Wheeler, How the Telegraph Helped Lincoln Win the Civil War, available at http://hnn.us/articles/30860.html; accessed March 20th, 2012

Gibson describes it as a "... 'consensual hallucination' of data experienced by billions of people worldwide…"[6] Twenty-four years after Gibson's publication, on May 12th, 2008, Deputy Undersecretary of Defense Gordon England defined *cyberspace* for the DoD in official correspondence as, "… a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[7] This definition remains as written in DoD Joint Publication 1-02. While the definition sounds straightforward, the attempt at any organized effort by the DoD to act upon it to secure U.S. vital interests and *provide for the common defense* against threats emerging from critical vulnerabilities in cyberspace has thus far been fraught with divergent interpretation and resulting confusion due to operational environment intricacies. This confusion has been exacerbated by the rapid growth of information technologies over a relatively short period of time, and the resulting reliance upon and interconnectedness of the very networks included in the definition.[8]

As a forcing mechanism, the 2010 Quadrennial Defense Review (QDR) established the requirement for DoD efforts to operate effectively in cyberspace and officially acknowledges that, "cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[9] Currently, at least 16 Joint Publications discuss cyber topics and at least 8 discuss *cyber operations*, but none of them

[6] Christopher J. Castelli, Defense Department Adopts New Definition of Cyberspace, available at http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm; accessed March, 20th 2012.
[7] Ibid.
[8] General Keith Alexander, Congressional Testimony on September 23, 2010, available at http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf, accessed on March 16, 2012.
[9] Secretary of Defense (former) Rober M. Gates, 2012 Quadrennial Defense Review Report, P. 37.

provide clarity in how to go about executing operations in cyberspace.[10] Not long after the 2010 QDR was published, the DoD took a step forward in organizing Departmental cyber efforts by standing up CYBERCOM – a measure that certainly creates some efficiency for the execution of these cyber operations. However, understanding the cyberspace operational environment sheds light on the requirement to do *more* to embolden the CYBERCOM command organization structure.

USCYBERCOM Mission and Operational Environment Necessitate COCOM status

The USCYBERCOM mission derives from a confluence of responsibilities formerly held by two DoD agencies subordinate to USSTRATCOM: the Joint Functional Component Command - Network Warfare (JFCC-NW) and the Joint Task Force - Global Network Operations (JTF-GNO), which were responsible for the offensive and defensive network operations respectively.[11] Given this, there is no surprise as to the two objectives on which USCYBERCOM focuses its efforts: *operate and defend defense networks* and, *on order, conduct offensive operations in cyberspace.*[12] These objectives bring about three interesting questions regarding the operational environment. Particularly, what is the operational environment as it relates to cyberspace and USCYBERCOM; and who are the potential adversaries against whom CDRUSCYBERCOM must conduct offensive and defensive operations; and what are the implications for the CDRUSCYBERCOM regarding the operational factors of *time, space, and force* as he prosecutes his mission set in this operational environment?

---

[10] United States Government Accountability Office Report to Congressional Requesters, Defense Department Cyber Effort: DOD Faces Challenges In Its Cyber Activities; available at http://www.gao.gov/assets/330/321818.pdf, accessed on March 21, 2012.
[11] General Keith Alexander, Congressional Testimony on March 16, 2011, available at http://www.dod.mil/dodgc/olc/docs/testAlexander03162011.pdf, accessed March 26, 2012.
[12] United States Strategic Command Fact Sheet, available at http://www.stratcom.mil/factsheets/Cyber_Command/, accessed March 13, 2012.

In answering the first question, one must understand how the DoD defines *cyberspace*. As the old adage goes, *words have meaning.* In the case of current U.S. DoD doctrinal terminology, many of the traditional terms simply do not apply to cyberspace operations and fail to capture the magnitude of the USCYERCOM mission set. The terms *operational environment* and *area of operations* assist in understanding the operational level of war for conventional mission sets and related objectives as they indicate spatial or other *measurable* boundaries to aid commanders in focusing their efforts in relation to their objectives. However, while the physical elements of cyberspace can be *roughly* measured, the interconnected global nature and the nuanced social component of the associated networks essentially makes the operational environment *immeasurable* – or, at least, makes the quantification of it irrelevant.

That is, the operational environment the CDRUSCYBERCOM deals with is, in a word, *global* – even its own domain. Demonstrating just how global these networks have become is best illustrated by some simple statistics: in 1995, there were 16 million users of the INTERNET; today, just over two decades later, there are over 2 billion internet users, all actively participating in cyberspace.[13] Even focusing on *just* the U.S. DoD's aspects of this construct becomes mind-boggling. The U.S. DoD "…operates 15,000 networks across 4,000 installations in 88 countries. We use more than 7 million computer devices. It takes 90,000 personnel and billions of dollars annually to administer, monitor and defend those networks. And yet the cyber threat continues to grow."[14] While these numbers provide some idea of the magnitude of cyberspace and demonstrate that a subordinate unified commander is

[13] http://www.internetworldstats.com/emarketing.htm
[14] Under Secretary of Defense William J. Lynn, III, speech given on January 21st, 2010 at the USAF-Tufts-Institute for Foreign Policy Analysis Conference, Washington, D.C., available at http://www.defense.gov/speeches/speech.aspx?speechid=1410, accessed March 25, 2012.

presently responsible for a global domain, these dimensions are not enough. The *threat* to DoD networks must be understood as well.

It is through appreciation of the threat then, that one develops a full understanding of the operational environment and level of war in cyberspace. In assessing the threat, there are really only two distinct categories under which potential threats fall: *state* and *non-state actors*. Both groups may be potential adversaries CDRUSCYBERCOM has to defend DoD networks against and against whom he may be ordered to take offensive action. Though not new, these threats have become increasingly more insidious as cyberspace has grown. The United States, and the DoD in particular, has seen the evolution of these threats and has become a central target. Three recent examples of cyber-attacks demonstrate the threat complexity of, possibilities in, and insight into the uniqueness of the cyberspace operational environment further drawing attention to the need for CYBERCOM to be a unified command.

First, in 2008, malware on an infected *thumb drive* found its way into a workstation connected to a U.S. Central Command network from a network computer physically located in the Middle East. In nanoseconds, this malicious code worked its way first thru UNCLASSIFIED and then CLASSIFIED DoD networks and created what former Undersecretary of Defense Lynn referred to as, "…a digital beachhead, from which data could be transferred to servers under foreign control…" and is acknowledged as the greatest breach of U.S. DoD computers ever.[15] An unwitting assistant facilitated this breach of existing defenses. A DoD service-member introduced the malware into the system by inserting an infected thumb drive into his workstation and the worm instantly propagated

[15] Under Secretary of Defense William J. Lynn, III, in an article written for the September/October Foreign Affairs Journal, available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain, accessed March 26, 2012.

across defense networks. The extent of the damage is classified, but the event clearly identified vulnerabilities in the DoD networks.

Second, the attack on Iranian nuclear power centrifuges in July of 2010 could be an extract from Richard Clarke's book *Cyber War* where he discusses the magnitude of offensive capabilities in cyberspace. The *Stuxnet* virus, as it has come to be known, uses malicious code to ultimately degrade Iranian nuclear power and nuclear weapons development process. It is a complex software program that exploits vulnerabilities in the Microsoft Windows Operating System that reportedly infected computers operating centrifuges at Iranian power plants – along with tens of thousands of computers worldwide, including some in the United States. Ultimately, the Iranian centrifuges were destroyed to some degree by this malicious code. "German expert Ralph Lagner describes Stuxnet as a military-grade cyber missile that was used to launch an 'all-out cyber strike against the Iranian nuclear program'." Perhaps one of the most disturbing aspects of *Stuxnet* is the fact that now, two years later, the origin of the Stuxnet virus is still unknown.[16] A second disturbing fact is that the virus is *still* propagating across cyberspace infecting computers and will do so until the code's internal *kill-date* of June, 24, 2012.[17]

Whole nations can be crippled simply through strokes on a computer keyboard. In this third example, occurring in April and May of 2007, Estonia was the victim of such a cyber-attack. Perhaps outraged over a politically charged decision to move a monument of a World War II-era Russian soldier from a park in Estonia, unknown parties launched a distributed denial of service (DDOS) attack against Estonian computer networks virtually,

[16] James P. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, in Survival: Global Politics and Strategy, Volume 53, Issue 1, 2011

[17] Elinor Mills, Stuxnet: Fact vs. Theory, available at http://news.cnet.com/8301-27080_3-20018530-245.html, accessed March 26, 2012.

and literally, shutting the nation down and taking it off the global information grid (GIG). The would-be cyber terrorists simply overwhelmed Estonian government, banking, and various other websites and computers with data causing a virtual gridlock and resulting denial of service. Though many in Estonia believe the attack was at least sanctioned by the Russian government, Russia has denied these claims.[18]

Much can be taken from these three examples of cyber warfare to understand USCYBERCOM's complex operational environment and a glimpse at the threat. Some general considerations based on these examples follow. First, any one of the two billion INTERNET users from any part of the world can be a potential threat. Second, the potential threats to DoD networks can come from within the physical borders of the United States – both physical threats and logical threats. Third, cyberspace creates significant challenges for attribution. No nation has claimed any responsibility for any of the myriad cyber-attacks that have occurred – though many argue that only a state-sponsored effort would have the means available to launch a *Stuxnet-like* attack. Lastly, the effects can be tremendously asymmetric – that is, one lone actor with the right code can have devastating national-level effects.[19]

While these threat considerations are extremely pervasive, there is much more that the CDRUSCYBERCOM must consider than the implications brought forth in the foregoing examples – all of which is exacerbate by his organization's command organization structure. In order to capture these in a coherent way, this work assesses them through the lenses of the operational factors of *time, space, and force* on USCYBERCOM's operational mission in attempt to demonstrate the unnecessary impediments resulting from USCYBERCOM's

[18] Mark Landler and John Markoff, Digital Fears Emerge After Data Siege in Estonia, available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1, accessed March 26, 2012.
[19] General Keith Alexander, in testimony before Congress on March 16, 2011, available at http://www.dod.mil/dodgc/olc/docs/testAlexander03162011.pdf, accessed March 26, 2012.

subordinate unified command status.

Considering Time, Space and Force Implications and Impediments

The eminent naval scholar Dr. Milan Vego's work *Joint Operational Warfare: Theory and Practice* brings particular insight to the importance for commanders to balance the factors of time, space, and force against the operational objective in order to give the operational commander freedom of action in the operational environment. Wisely, he draws attention to his position that this process is much more of an *art* than it is a science.[20]

Vego refers to *space* as both a quantifiable means and an objective and acknowledges that there are considerable differences between the traditional view of operational space and cyberspace – primarily the fact that the physical environment in cyberspace is practically limitless.[21] Even so, securing cyberspace for DoD freedom of action is inherent in USCYBERCOM's mission. As General Keith Alexander, CDRUSCYBERCOM, states, "Making our access to cyberspace impossible or even problematic would represent a strategic threat to America's vital interests—one that our Command has been established and tasked to prevent with respect to DoD's operations in the cyberspace." This access is inextricably linked to allied nations, commercial interests, the U.S. Interagency (including the NSA and the Department of Homeland Security in particular) and is potentially threatened by users and/or systems that can be physically located anywhere in the world, including inside the United States.[22] The globally interconnected nature of the commercial networks to which the DoD infrastructure is linked allows state or non-state actors to use networked routers and switches that are physically located within U.S. borders, or most any other nations for that

[20] Milan Vego, Joint Operational Warfare: Theory and Practice. Newport, RI: Naval War College, reprint, 2009. Pp. III-3 – III -63.
[21] Ibid, III-15.
[22] General Keith Alexander, Congressional Testimony on March 16, 2011, available at http://www.dod.mil/dodgc/olc/docs/testAlexander03162011.pdf, accessed March 26, 2012.

matter, to carry out their cyber-attacks. This brings about unique coordination and cooperation requirements between USCYBERCOM and a plethora of partners – from the Services and all DoD Functional and Geographic Combatant Commanders to counterparts in allied nations, and the Interagency. General Alexander calls attention to the required strengthening of these *partnerships* in order to better achieve his objectives.[23] As such, USSTRATCOM provides an unnecessary layer of oversight and bureaucracy that reduces efficiency in bringing these relationships about.

As Dr. Vego identifies, "… space lost can be regained; time lost can never be recovered."[24] Typical operational considerations for maneuver forces regarding time revolve around more tangible issues such as time to train, equip, and transport or build-up forces, the advantages a commander might gain or lose by taking more timely actions, or the timing of tactical actions to gain a particular effect over an adversary. Regarding the USCYBERCOM mission, these considerations are largely irrelevant. The fact is that DoD networks are attacked over 250,000 times… *per hour*.[25] In this environment, the enemy moves at the speed of light. Understanding the cyberspace operational environment, it becomes even more critical that the CDRUSCYBERCOM be able to act faster than any adversary. Essential to this is the ability to reduce time required for planning and the reduction of the length of the decision-making cycle.[26] There is but one way to do this to the magnitude required. The myriad entities involved in the prosecution of DoD network defense (as previously listed) or to take offensive action in cyberspace necessitates a direct line and

[23] Ibid.
[24] Milan Vego, Joint Operational Warfare: Theory and Practice. Newport, RI: Naval War College, reprint, 2009. Pg. III-19.
[25] General Keith Alexander, Congressional Testimony on September 23, 2010, available at http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf, accessed on March 16, 2012.
[26] Ibid. Pp. III-19, III-24.

equality between the CDRUSCYBERCOM and those entities' leaders. Given the requirement for Subordinate Unified Commanders top keep their higher headquarters abreast of developing issues, USSTRATCOM provides an unnecessary layer of bureaucracy.

In considering the factor of force, much of what Dr. Vego discusses in his monumental work on the matter provides little value concerning cyberspace operations - although an argument could certainly be made to the contrary. Nevertheless, there is one tangible element included in the factor of force that greatly contributes to the transfer of combat potential, or the theoretical power of a given military element, into combat power, or the actual combat capability in a given operational environment.[27] The most perplexing aspects of force assessment are the nuanced subtleties, deemed *intangibles,* which are difficult to quantify.[28] Vego states that *command organization* has a *considerable* effect on the ability to transfer combat potential to combat power.[29] This brings about implications from Joint Publication 1 – specifically the doctrinal principles that guide Joint Force command and control, the primary in question being *span of control.* The following is the doctrinal guideline for considering *span of control* as it relates to Joint Force Commanders (JFC).

> "The desired reach of the JFC's authority and direction over assigned or attached forces will vary depending on the mission and the JFC's ability to C2 the actions required. Span of control is based on many factors including the number of subordinates, number of activities, range of weapon systems, force capabilities, the size and complexity of the operational area, and the method used to control operations (centralized or decentralized)."[30]

[27] Ibid., Pp. III-33 - III-40
[28] Ibid. Pg. III-35
[29] Ibid. Pg. III-40
[30] Joint Publication 1, Pg. IV-19.

The focus here is not CDRUSCYBERCOM. Rather it is CDRUSSTRATCOM's ability to effectively provide oversight of the magnitude of missions under USSTRATCOM, of which USCYBERCOM's is included. Relying on Vego's acknowledgement that this particular area is difficult to quantify, a *qualification* is then required. Simply put, commanders must prioritize effort based on the greatest threat. To what degree, then, is the profound mission of USCYBERCOM *the* top priority for CDRUSSTRATCOM. By his own admission, it is not. The following provides perspective on the magnitude of missions for which General Kehler is responsible and his priority of effort.

> "As the USSTRATCOM Commander, I am assigned responsibilities in the broader nuclear enterprise as well. I am a member of the Nuclear Weapons Council, and I lead the combatant command responsible for nuclear capability advocacy. Furthermore, I am responsible for annually certifying to the President the surety of the nation's nuclear weapons stockpile. Finally, I provide professional military advice to the President, the Secretary of Defense, and the Chairman of the Joint Chiefs of Staff on nuclear strategy, operations, and weapons issues. Given the magnitude of these responsibilities and the continuing importance of nuclear weapons in our national security posture, USSTRATCOM's number one priority remains to ensure we have a safe, secure, and effective nuclear deterrent force and to operate that force to deter attack on the U.S. and our allies."[31]

So then, the argument is a simple one: to what degree will USCYBERCOM be denied resources for the sake of USSTRATCOM's nuclear mission? While there is a lingering threat of nuclear weapons of mass destruction being used against the United States, there is a very strong argument to be made that the threat of cyber-attack greatly overshadows this potential. The U.S. is being attacked in cyberspace *right now*.

There is a second, more direct impediment related to the operational factor *forces* and command organization given an understanding of the foregoing - CDRUSCYBERCOM's

[31] General Robert Kehler, Congressional Testimony, November 2, 2011, available at http://www.stratcom.mil/speeches/2011/76/Statement_Before_the_House_Committee_on_Armed_Services_Subcommittee_on_Strategic/, accessed March 27, 2012.

command authority is insufficient given the magnitude of his mission and operational environment. As a subordinate unified commander, CDRUSCYBERCOM can only be delegated operational control (OPCON) of his forces. As discussed in Joint Publication 1, there are significant differences between combatant command (COCOM) command authority, which is bestowed upon a unified commander by Title 10 U.S. Code, and OPCON of forces. With OPCON authority, the CDRUSCYBERCOM only has the ability to "perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission".[32] At face value this may seem sufficient, but there is a great deal more the commander needs to better accomplish his objectives. COCOM authority establishes the unified commander as the "…US military single point of contact and exercise directive authority over all elements of the command in relationships with other combatant commands, DOD elements, US diplomatic missions, other US agencies, and organizations of other countries…"[33] Further, COCOM authority allows the commander to "…coordinate with other CCDRs, USG agencies, and organizations of other countries regarding matters that cross the boundaries of geographic areas specified in the UCP and inform USG agencies or organizations of other countries in the AOR, as necessary, to prevent both duplication of effort and lack of adequate control of operations in the delineated areas."[34] Given the limitless *space* in which cyber operations occur, this authority is critical. Next, the ability to assess budget limitations of assigned forces and directly impact the budget request process for assigned forces is retained under COCOM authority. This limits ability to equip assigned forces for mutually supporting efforts or to

[32] Joint Publication 1, Pp. IV-7 – IV-8.
[33] Ibid., Pg. IV-5.
[34] Ibid., Pg. IV-4.

standardize response processes based on standardized equipment throughout the command. Finally, COCOM authority includes directive authority for logistics. This "…includes the authority to issue directives to subordinate CDRs, including peacetime measures necessary to ensure the following: effective execution of approved OPLANs; effectiveness and economy of operation; and prevention or elimination of unnecessary duplication of facilities and overlapping of functions among the Service component commands."[35] Taken as a whole, the authorities CDRUSCYBERCOM *does not have* as a subordinate unified commander provide tremendous impediments in working across the Services, the Interagency, and even internationally, combined with the inability to control budget allocation, subordinate unit organization and the like provide extreme limitations on CDRUSCYBERCOM given the mission and operational environment.

Counterargument

While there is no standing argument that refutes what research has demonstrated in this work, there is a resounding argument that the intangible implications impeding CDRUSCYBERCOM due to his status as a subordinate unified commander do not justify adding another unified command to the U.S. DoD. *Money* is the central theme to this argument. Critics, such as Nathan Freier, Senior Fellow at the Center for Strategic and International Studies, argue that resource constraints must drive the DoD to reduce unified commands, not increase them. Particularly condemning comments published about the 2011 Unified Command Plan (UCP) provide insight. In his review, Freier conveys that the DoD has had the pleasure of unrestricted budgets over the last decade, which has resulted in a significant growth for four-star commands and multiple unified commands – specifically

[35] Ibid., Pg. IV-6

United States Northern Command in 2002 and United States Africa Command in 2008.[36] To add, Freier targets the notion of *span of control* as the last bastion of hope to maintain many of the existing unified commands. He writes, "How, for example, is a single command going to manage engagement with all the countries of Europe and Africa combined? The response is as uncomfortable as it is necessary. As resources decline… four-star commanders will increasingly need to allocate resources and effort according to consideration of what absolutely must and can be done with what's on hand and not what could and might be done with additional time and money."[37]

While these arguments have merit, they are more of a challenge to DoD leadership to prioritize efforts and create efficiencies where required in order to create room for USCYBERCOM as a unified command. There are two primary ways to do this – perhaps one less transformational than the other. First, DoD leadership could reorganize and combine COCOMs to downsize in order to reduce costs. In this, both United States European Command (USEUCOM) and United States Africa Command (USAFRICOM), and United States Southern Command (USSOUTHCOM) are prime targets for realignment based on threat assessments from these areas. A second approach is to completely dissolve the COCOM model and replace this legacy construct with a structure that better incorporates a whole-of-government approach to regional issues rather than breaking down the world into areas on which senior military commanders plan military response to potential threats. U.S. Congress is entertaining both potential courses of action. [38]

---

[36] Nathan Freier, The 2011 Unified Command Plan – A Missed Opportunity, May 24, 2011. Available at http://csis.org/publication/2011-unified-command-plan-missed-opportunity, accessed on March 27, 2012.
[37] Ibid.
[38] Andrew Feickert, The Unified Command Plan and Combatant Commands: Background and Issues for Congress, available at http://www.fas.org/sgp/crs/natsec/R42077.pdf, accessed April 3, 2012.

Summary and Recommendations

While money is a current concern, it is clear that cyberspace and the critical vulnerabilities therein will only become more intertwined with U.S. national interests as time progresses. As a result, the USCYBERCOM mission rivals that of any existing unified command and surpasses the existing missions of some standing COCOMs. The cyberspace operational environment, now its own domain, is essentially limitless and permeates the platforms and forces that exist in sea, air, land, and space domains. To add, the considerations of time, space, and force (in particular), drive home the tangible and intangible impediments facing the CDRUSCYBERCOM. It is only after understanding the mission and operational environment that one can appreciate these impediments. Perhaps the most significant of these is the recognition that the critical cyber mission is simply not *the* top priority for USCYBERCOM's parent COCOM. These things, combined with the inability for CDRUSCYBERCOM to organize, train, and equip his forces due to lack of COCOM authority brings about a confluence of factors that further demonstrates the need for USCYBERCOM to be a unified command to better accomplish its objectives.

Recommend DoD leaders assess and adopt one of two viable courses of action to bring about this necessary change while considering the significant fiscal constraints that will exist for the foreseeable future. First, DoD leadership could realign the existing unified commands to allow for USCYBERCOM to transition to unified command status based on costs savings gained from the realignment. Second, leadership could take a more transformational approach and develop a new Joint Task Force construct that replaces the Geographic Combatant Commands, streamlines the threat/response process and allows USCYBERCOM to emerge as a *functional* unified command.

Bibliography

Castelli, Christopher J. "Defense Department Adopts New Definition of Cyberspace", available at http://integrator.hanscom.af.mil/2008/May/05292008/05292008-24.htm (accessed March, 20th 2012)

Farwell, James P. and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War", in *Survival: Global Politics and Strategy*, Volume 53, Issue 1, 2011.

Freier, Nathan. "The 2011 Unified Command Plan – A Missed Opportunity", May 24, 2011. available at http://csis.org/publication/2011-unified-command-plan-missed-opportunity (accessed on March 27, 2012)

Feickert, Andrew. "The Unified Command Plan and Combatant Commands: Background and Issues for Congress", available at http://www.fas.org/sgp/crs/natsec/R42077.pdf (accessed April 3, 2012)

General Alexander, Keith, *Congressional Testimony on March 16, 2011*, available at http://www.dod.mil/dodgc/olc/docs/testAlexander03162011.pdf, accessed March 26, 2012.

General Alexander, Keith, *Congressional Testimony on September 23, 2010*, available at http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC%20Command%20Posture%20Statement_HASC_22SEP10_FINAL%20_OMB%20Approved_.pdf (accessed on March 16, 2012)

General Kehler, Robert, *Congressional Testimony, November 2, 2011*, available at http://www.stratcom.mil/speeches/2011/76/Statement_Before_the_House_Committee_on_Armed_Services_Subcommittee_on_Strategic/ (accessed March 27, 2012)

Internet World Stats, available at http://www.internetworldstats.com/emarketing.htm, (accessed on March 21, 2012)

Landler, Mark and Markoff, John, Digital Fears Emerge After Data Siege in Estonia, available at http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1, (accessed March 26, 2012)

Mills, Elinor, Stuxnet: Fact vs. Theory, available at http://news.cnet.com/8301-27080_3-20018530-245.html (accessed March 26, 2012)

U.S Government Accountability Office. *Report to Congressional Requesters, Defense Department Cyber Effort: DOD Faces Challenges In Its Cyber Activities*, available at http://www.gao.gov/assets/330/321818.pdf (accessed on March 21, 2012)

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: CJCS, 2 May 2007 amended through 20 March 2009, Pp. IV-1 – IV-19.

U.S. President Obama, Barrack, *2010 National Security Strategy*, P. 28.

U.S. Secretary of Defense Gates, Robert M. *2012 Quadrennial Defense Review Report*, Pg. 37.

U.S. Strategic Command Fact Sheet, available at http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed March 13, 2012)

U.S. Under Secretary of Defense Lynn, William J. III, speech given on May 22nd, 2010 at the STRATCOM Cyber Symposium, Omaha, NE, available at http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1 (accessed March 12, 2012)

U.S. Under Secretary of Defense Lynn, William J. III, in an article written for the September/October Foreign Affairs Journal, available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (accessed March 26, 2012)

U.S. Under Secretary of Defense Lynn, William J. III, speech given on January 21st, 2010 at the USAF-Tufts-Institute for Foreign Policy Analysis Conference, Washington, D.C., available at http://www.defense.gov/speeches/speech.aspx?speechid=1410, accessed March 25, 2012.

Vego, Milan, *Joint Operational Warfare: Theory and Practice*. Newport, RI: Naval War College, reprint, 2009.

Wheeler, Tom, *How the Telegraph Helped Lincoln Win the Civil War*, available at http://hnn.us/articles/30860.html (accessed March 20th, 2012)